ABSTRAK

Penelitian ini bertujuan untuk menerapkan algoritma paillier cryptosystem untuk enkripsi dan dekripsi citra yang bereksistensi *.bmp, *.jpg, atau *.png serta menguji tingkat keamanan algoritma paillier cryptosystem. Algoritma paillier cryptosystem digunakan karena komputasi enkripsi pada algoritma paillier cryptosystem cukup rumit, karena diperlukan dua kali operasi perpangkatan, satu kali operasi perkalian, dan satu kali operasi modulo. Dengan demikian tingkat keamanan algoritma paillier cryptosystem cukup baik. Hasil penelitian menunjukkan bahwa jika nilai p dan q yang diinputkan saat pembangkitan kunci lumayan besar dan ukuran file citra yang akan diinputkan cukup besar maka waktu enkripsi akan memerlukan waktu yang lebih lama. Hasil pengujian keamanan algoritma berdasarkan analisis histogram dan analisis koefisien korelasi menunjukkan bahwa tingkat keamanan algoritma ini cukup baik karena histogram hasil enkripsinya cukup berbeda dari plain image, serta piksel-piksel pada hasil enkripsi sudah tidak memiliki korelasi satu sama lain.

Kata Kunci : *Kriptografi, Gambar, citra, algoritma Paillier Cryptosystem*

Abstract

*The purpose of the research is to use paillier cryptosystem algorithm for encryption and decryption image with *.bmp, *.jpg, or *.png. existence and testing the level of security of paillier cryptosystem algorithm. Paillier cryptosystem algorithm is used because the computation of encryption in paillier cryptosystem is quite complicated, since it requires two operation of squared, one operation of multiplication, and one operation of modular. So, the level of security is good enough. Result of research shows if p and q which are inputted while generator key's process is too big and the size of image file which is inputted is big enough, so the encryption's time will need more time. Result of testing the level of algorithm's security experiment by histogram analysis and correlation coefficient analysis shows that the level of security for this algorithm is good enough, because the encryption histogram's result looks different enough than the histogram's plain image, and the pixels in cipher image has not been correlation each other.*

Keyword : *Cryptography, Image, Paillier Cryptosystem Algorithm*